Message from the CIO

This semester has been another fall full of activity on campus, including the TTU IT Division. In this issue, we detail two new service enhancements: a change to TechMail delivery and the “AskIT” self-help IT resource for the campus community. In addition, we provide clarification about published directory information at TTU, as well as highlight the importance of Network Site Coordinators. We ask that you take a few minutes to review these services and updates and welcome your feedback—contact information is included in each article. We highly value your collaboration as we work to secure information resources and provide services to support the academic and research mission of our institution.

- Sam Segran
Associate Vice President for IT and Chief Information Officer

Change to TechMail Delivery

You may be aware, TechMail inserts an anti-phishing warning message into incoming email messages that spam filters identify as possible phishing attempts (a deceptive technique used by cyber criminals to entice you to voluntarily provide personal information and/or login credentials). We still have TTU faculty, staff, and students that fall prey to phishing schemes and as a result, TechMail services are interrupted for all. The inserted warning message reads:

WARNING: This message is not from a sender on your Safe Sender’s list AND MAY BE AN ATTEMPT TO STEAL YOUR PASSWORD. No email from a reputable source will ever ask for, or direct you to verify, your email account information! If you are certain of the sender’s identity and need to reply or forward this message, delete this warning verbiage before sending and add the address to your Safe Sender’s list.

For further assistance, call (806) 742-4357.

In the past, any incoming email that had this warning message inserted was automatically placed in the recipient’s Junk Mail folder. **As of last month, incoming email that has the warning message inserted will not automatically be placed into Junk Mail and will appear in your Inbox.**

This change should help alleviate reported issues with legitimate/business email being placed into Junk Mail folders.

Since TechMail spam/phishing filtering is affected by various server and client strategies, please note that:

- TTU IT strongly recommends that you actively maintain your Safe Senders List – email from Safe Senders is not affected by spam/phishing filters;
- Any email from a sender not on your Safe Senders list could still be scored as spam and delivered to your Junk Mail folder, including email with the anti-phishing warning message. To prevent this, add the sender to your safe sender list;
- No spam filter or anti-spam strategy is ever accurate 100% of the time, so you should check your Junk Mail folder regularly for any email that filters have incorrectly identified as spam;
- All email older than 30 days is automatically deleted from your Junk Mail folder; and
- In addition to spam filtering performed by TechMail servers, your email client can be used for additional spam filtering or for establishing custom rules that can direct your incoming mail to specific folders.

Phishing attempts are becoming increasingly difficult to detect. The TTU IT Division recommends the following best practices to help protect your personal information, as well as University information resources:

- Do not respond to emails that ask you to provide your personal information or your login username/passwords;
- Avoid clicking on links provided in emails, unless you are certain the link is to a legitimate and authentic website;
- Be aware that phishing emails are designed to look authentic, often using “official” company logos/text and appearing to come from a legitimate source; and
- Cyber criminals that obtain your email account credentials (i.e. username/password) can use your email account to send spam and malware to your friends and family (via your Contacts List), and potentially to thousands of email addresses all over the world.

For additional information regarding email and anti-spam/phishing filtering, please contact IT Help Central at (806)742-4357 (HELP), by email at ithelpcentral@ttu.edu, or visit our website at www.ithelpcentral.ttu.edu.

Help at Your Fingertips: www.askIT.ttu.edu

After months of planning and extensive testing, the TTU IT Division has launched a new self-help resource for information technology assistance. AskIT allows you to use the same knowledge base that IT Help Central uses to resolve customer issues. You will also be able to use askIT to view a list of scheduled maintenance and known system outages, as well as view your own technical issues, update them, or close them.

AskIT has two primary interfaces:

**Guest Portal (Open to the general public)**
- Guests are able to search or browse approximately 1,500 custom solutions from IT Help Central’s currently internal-only knowledge base.
- Guests can also open a new issue with IT Help Central.

**Authenticated Portal (Open to anyone with an eRaider account)**
- Contains everything in Guest Portal, plus:
  - Search IT Help Central knowledge base solutions which require eRaider authentication to view (such as security-sensitive items)
  - Search 60,000+ additional knowledge base solutions from RightAnswers, a company that specializes in IT knowledge management
  - View a list of current system outages and scheduled maintenance periods
  - View issue notes and other details for your current and previous issues
  - Close your own issues or add notes to them

We invite you to use the askIT service at www.askit.ttu.edu. For any questions or additional information about askIT, please contact IT Help Central at (806)742-HELP (4357) or via e-mail at ithelpcentral@ttu.edu.
Understanding Directory Information

Texas Tech University carefully complies with all state and federal regulations regarding your personal information. It is important to understand that these databases are distinct.

TechAlert – The Emergency Notification Database

The TTU IT Division Application Development and Support area collaborated with TTU Communications and Marketing, as well as the Office of the President, to create a standalone database for faculty, staff, and students to maintain their emergency contact information. TechAlert is not linked to any other data source on campus. By visiting www.emergency.ttu.edu and clicking the “Get the Message” link, you can log in with your eRaider account and review your emergency contact information. Note that by policy, the TechAlert database can ONLY be used for emergency notification and is never published or released.

The Global Address List (GAL)

The GAL is viewable from Outlook and is the internal working business directory for students, employees, and other authorized individuals. This directory is populated from data sent nightly from Banner information systems and is not available to the general public. Previous discussions with TTU General Counsel and the CIOs from all TTU institutions concluded that a minimum amount of information must be available in this internal business directory in order to uniquely identify and contact students and employees. No information appears in this directory beyond name and email address for students who have unchecked the “Display in Directory” flag in Raiderlink under “Directory Profile.” For students who have checked this flag, only name, email, address, and phone number would appear. For students who may also be employees, a business phone number and business address may also appear. Any student or employee also may elect to add additional information to the directory using www.eraider.ttu.edu.

Online Directory

The TTU online directory (http://info.ttu.edu) includes basic contact information for employees and does not include student information.

We encourage you to review your information in these directories. For any questions or additional information about directory information, please contact IT Help Central at (806)742-HELP (4357) or via e-mail at ithelpcentral@ttu.edu. If you have questions regarding any information that has been released, you may contact the Registrar at http://www.depts.ttu.edu/registrar/default.aspx and click on the “Contact Us” link on the left navigation pane.

Importance of Network Site Coordinators and a New IT Resource

Texas Administrative Code Rule §202.71(c) states that all custodians of information resources shall be identified by each institution. In essence, the rule requires all TTU departments to assign personnel responsible for maintaining the security of area computing environments. This role designation, known as a Network Site Coordinator (NSC), can solidify paths of communication between departments and TTU IT Division resources on issues that affect the computing infrastructure, such as performance and security. It is important that all areas, regardless of size, understand importance of designating an employee that can be a liaison between the department and the IT Division.

The TTU Security Operations Center, in coordination with TTU IT compliance efforts, will be communicating with all area NSCs on the use of an important tool for protecting the TTU computing infrastructure. This tool called QualysGuard, scans networked servers, workstations, laptops, and printers for security vulnerabilities—gaps that make computing equipment susceptible to malware and hacking attempts.

If you are a department head, please take a moment to remind your NSC about the importance of taking advantage of QualysGuard for your area. If you have not appointed an NSC or your NSC designee has changed, please take the time to appoint one or to update the information. You can do so by completing the Network Site Coordinator Appointment Form located at www.net.ttu.edu/script/docs/nscform.asp. If you have questions about the role of the NSC or using the form, please contact IT Help Central at (806)742-HELP (4357) or via e-mail at ithelpcentral@ttu.edu.

Scanning the barcode to view IT Bulletins online

www.infotech.ttu.edu/itbulletin